Best Practices for Securing Your Data and Devices

Jeff Giacobbe
Assistant VP Enterprise Technology Services
giacobbej@mail.montclair.edu

Brian Beckett
Director of Systems and Security
beckettb@mail.montclair.edu

1

Best Practices for Securing Your Data and Devices

HELLO, THIS IS THE DOGBERT MARKET RESEARCH COMPANY. MAY I ASK YOU SOME TOTALLY HARMLESS QUESTIONS?
WHAT IS YOUR SOCIAL SECURITY NUMBER, BANK PIN NUMBER AND MOTHER'S MAIDEN NAME?
WHAT EXACTLY ARE YOU RESEARCH-ING?
POVERTY RATES. I'M SHOOTING FOR 100%.
Dilbert.com DilbertCartoonist@gmail.com
© 2010 Scott Adams, Inc./Dist. by UFS, Inc.

2

Goals for Today's Talk

- Overview of best practices for securing sensitive data on University-provided computers
- Recommendations for what **you can do today** to protect sensitive data you collect and manage
- A brief overview of some of the advanced techniques for data protection that could be implemented in the future with assistance from Information Technology

3

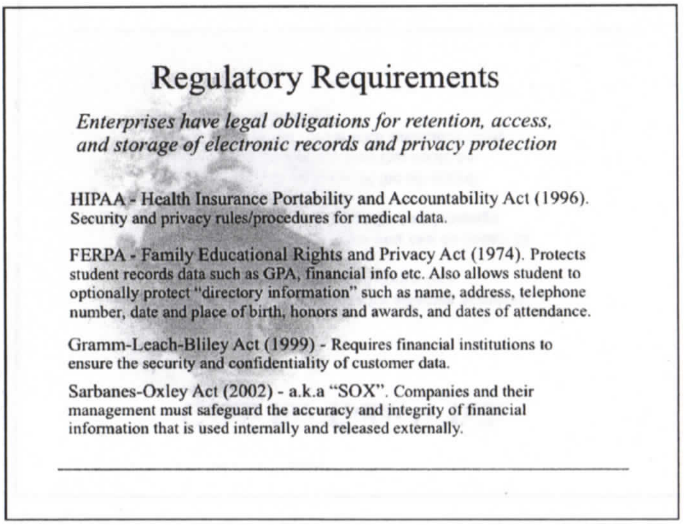
Let's define "sensitive" data

In general, data classification is the responsibility of the institution and is based on:

- Applicable internal policies
- State or Federal regulatory requirements
- Industry specific standards
- Other agreements between entities exchanging data

Information Technology is working on a data classification policy to augment the Responsible Use of University Computing Resources policy document.

4



Regulatory Requirements

Enterprises have legal obligations for retention, access, and storage of electronic records and privacy protection

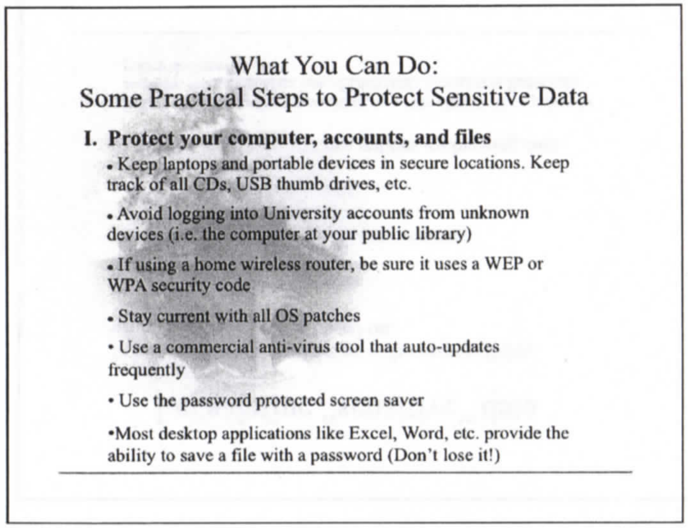
HIPAA - Health Insurance Portability and Accountability Act (1996). Security and privacy rules/procedures for medical data.

FERPA - Family Educational Rights and Privacy Act (1974). Protects student records data such as GPA, financial info etc. Also allows student to optionally protect "directory information" such as name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.

Gramm-Leach-Bliley Act (1999) - Requires financial institutions to ensure the security and confidentiality of customer data.

Sarbanes-Oxley Act (2002) - a.k.a "SOX". Companies and their management must safeguard the accuracy and integrity of financial information that is used internally and released externally.

5

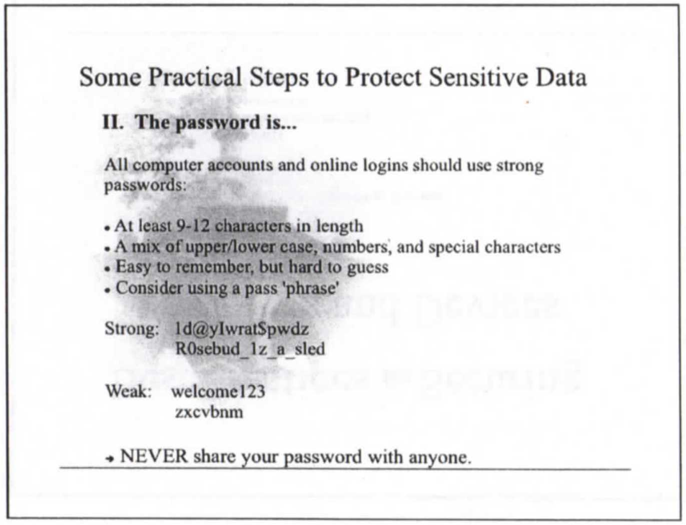


What You Can Do: Some Practical Steps to Protect Sensitive Data

I. Protect your computer, accounts, and files

- Keep laptops and portable devices in secure locations. Keep track of all CDs, USB thumb drives, etc.
- Avoid logging into University accounts from unknown devices (i.e. the computer at your public library)
- If using a home wireless router, be sure it uses a WEP or WPA security code
- Stay current with all OS patches
- Use a commercial anti-virus tool that auto-updates frequently
- Use the password protected screen saver
- Most desktop applications like Excel, Word, etc. provide the ability to save a file with a password (Don't lose it!)

6



Some Practical Steps to Protect Sensitive Data

II. The password is...

All computer accounts and online logins should use strong passwords:

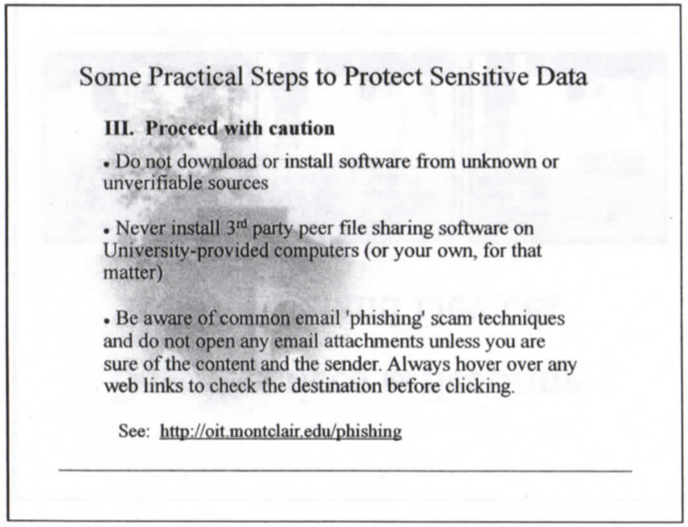
- At least 9-12 characters in length
- A mix of upper/lower case, numbers, and special characters
- Easy to remember, but hard to guess
- Consider using a pass 'phrase'

Strong: 1d@yIwrat$pwdz
R0sebud_1z_a_sled

Weak: welcome123
zxcvbnm

→ NEVER share your password with anyone.

7



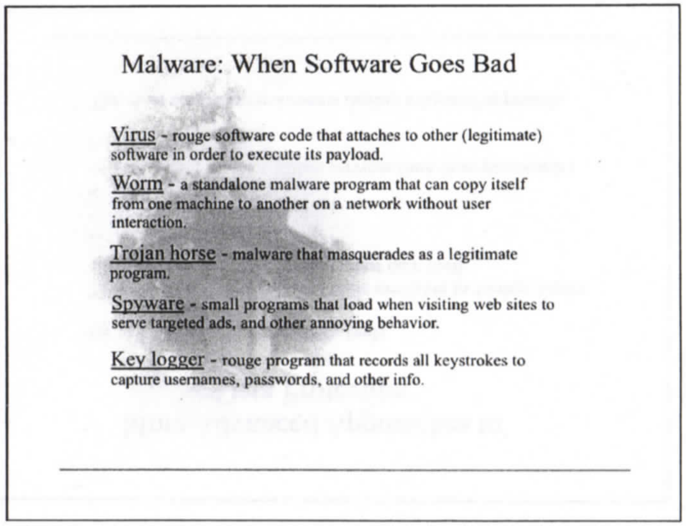
Some Practical Steps to Protect Sensitive Data

III. Proceed with caution

- Do not download or install software from unknown or unverifiable sources
- Never install 3rd party peer file sharing software on University-provided computers (or your own, for that matter)
- Be aware of common email 'phishing' scam techniques and do not open any email attachments unless you are sure of the content and the sender. Always hover over any web links to check the destination before clicking.

See: http://oit.montclair.edu/phishing

8



Malware: When Software Goes Bad

Virus - rouge software code that attaches to other (legitimate) software in order to execute its payload.

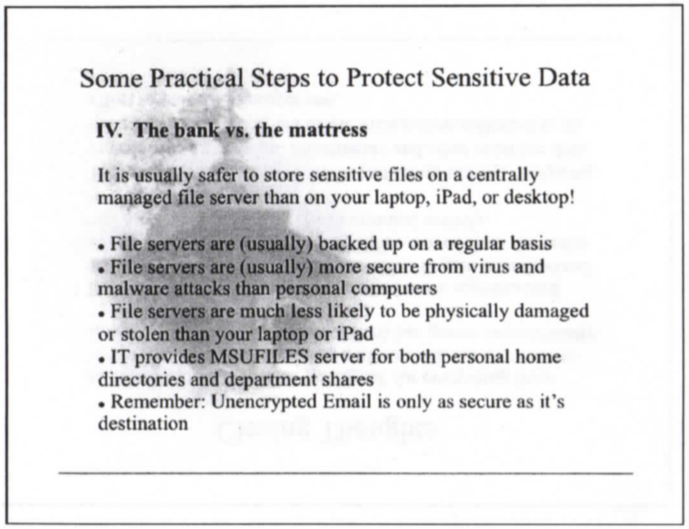
Worm - a standalone malware program that can copy itself from one machine to another on a network without user interaction.

Trojan horse - malware that masquerades as a legitimate program.

Spyware - small programs that load when visiting web sites to serve targeted ads, and other annoying behavior.

Key logger - rouge program that records all keystrokes to capture usernames, passwords, and other info.

9



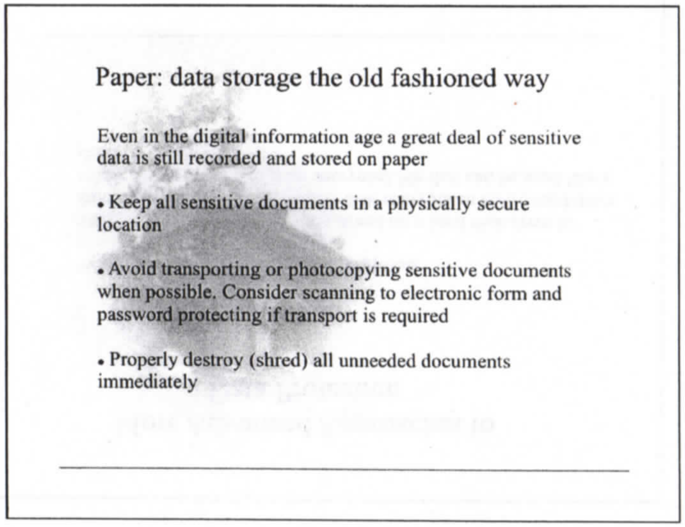
Some Practical Steps to Protect Sensitive Data

IV. The bank vs. the mattress

It is usually safer to store sensitive files on a centrally managed file server than on your laptop, iPad, or desktop!

- File servers are (usually) backed up on a regular basis
- File servers are (usually) more secure from virus and malware attacks than personal computers
- File servers are much less likely to be physically damaged or stolen than your laptop or iPad
- IT provides MSUFILES server for both personal home directories and department shares
- Remember: Unencrypted Email is only as secure as it's destination

10

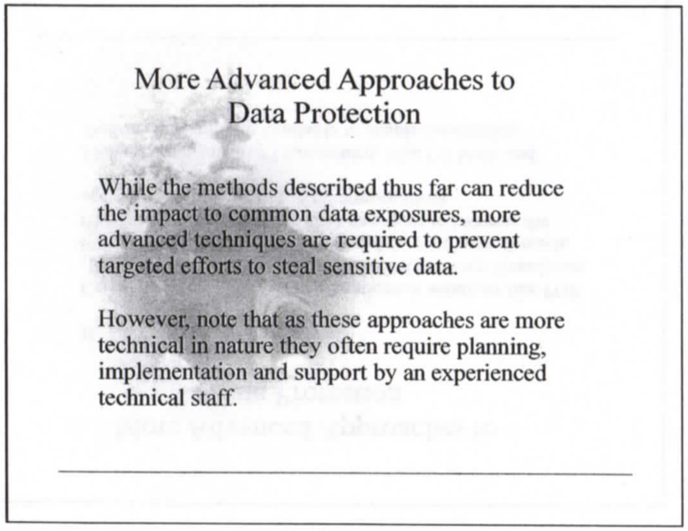


Paper: data storage the old fashioned way

Even in the digital information age a great deal of sensitive data is still recorded and stored on paper

- Keep all sensitive documents in a physically secure location
- Avoid transporting or photocopying sensitive documents when possible. Consider scanning to electronic form and password protecting if transport is required
- Properly destroy (shred) all unneeded documents immediately

11

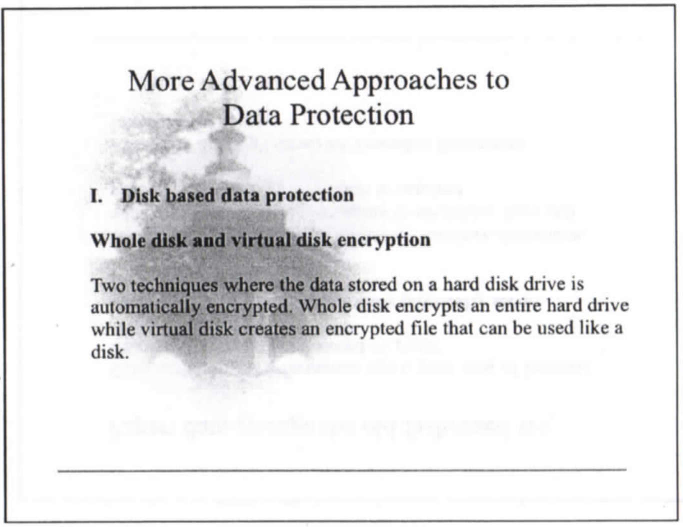


More Advanced Approaches to Data Protection

While the methods described thus far can reduce the impact to common data exposures, more advanced techniques are required to prevent targeted efforts to steal sensitive data.

However, note that as these approaches are more technical in nature they often require planning, implementation and support by an experienced technical staff.

12



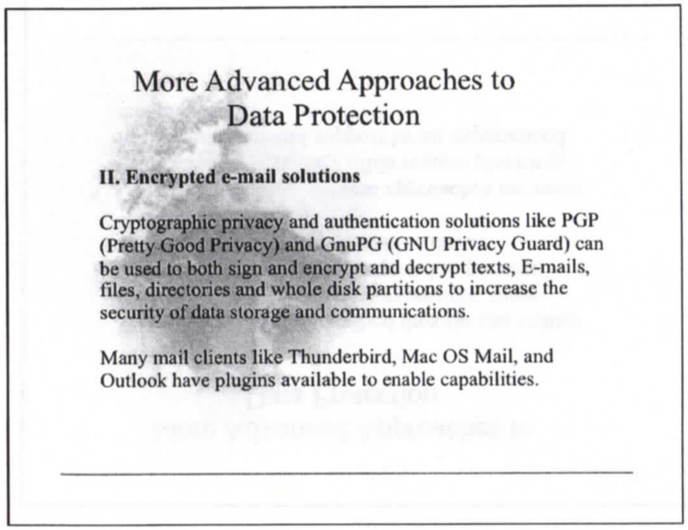
More Advanced Approaches to Data Protection

I. Disk based data protection

Whole disk and virtual disk encryption

Two techniques where the data stored on a hard disk drive is automatically encrypted. Whole disk encrypts an entire hard drive while virtual disk creates an encrypted file that can be used like a disk.

13



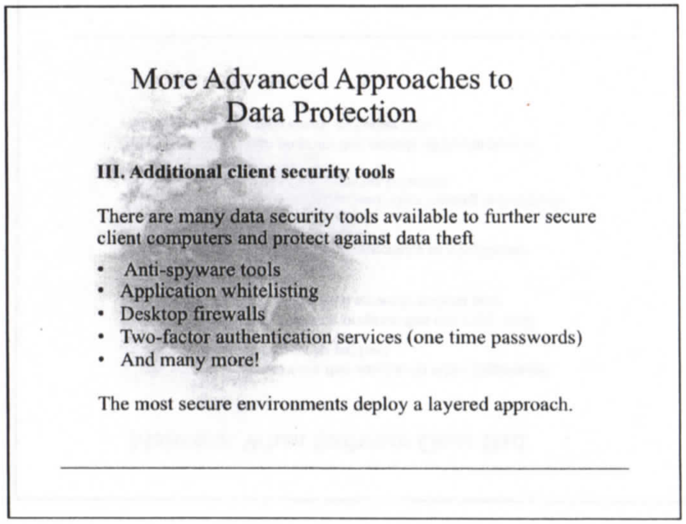
More Advanced Approaches to Data Protection

II. Encrypted e-mail solutions

Cryptographic privacy and authentication solutions like PGP (Pretty Good Privacy) and GnuPG (GNU Privacy Guard) can be used to both sign and encrypt and decrypt texts, E-mails, files, directories and whole disk partitions to increase the security of data storage and communications.

Many mail clients like Thunderbird, Mac OS Mail, and Outlook have plugins available to enable capabilities.

14



More Advanced Approaches to Data Protection

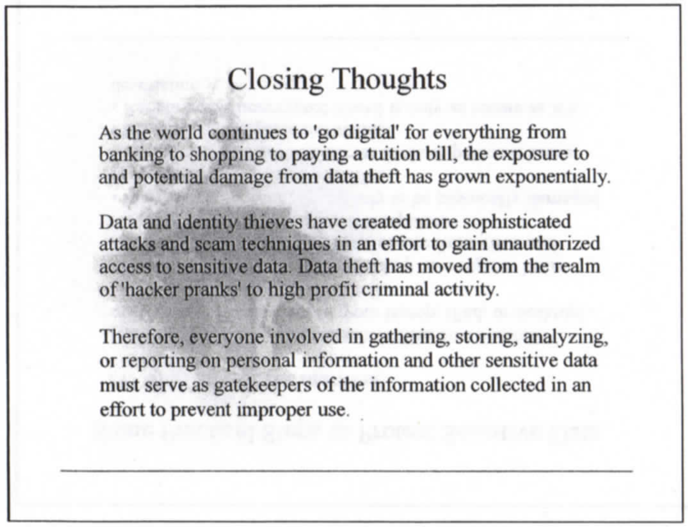
III. Additional client security tools

There are many data security tools available to further secure client computers and protect against data theft

- Anti-spyware tools
- Application whitelisting
- Desktop firewalls
- Two-factor authentication services (one time passwords)
- And many more!

The most secure environments deploy a layered approach.

15



Closing Thoughts

As the world continues to 'go digital' for everything from banking to shopping to paying a tuition bill, the exposure to and potential damage from data theft has grown exponentially.

Data and identity thieves have created more sophisticated attacks and scam techniques in an effort to gain unauthorized access to sensitive data. Data theft has moved from the realm of 'hacker pranks' to high profit criminal activity.

Therefore, everyone involved in gathering, storing, analyzing, or reporting on personal information and other sensitive data must serve as gatekeepers of the information collected in an effort to prevent improper use.

16

Slide 1

About the presenters

Combined, Jeff and Brian have over 40 years of experience in the field of computer technology with a wide range of experience and expertise in systems engineering, data center environments, project management, and computer security.

Both are also alumni of Montclair State University.

Slide 4

Many standards, such as the classification of data as **Personally Identifiable Information (PII),** are widely accepted but not universally consistent.

For example, Montclair State University follows the requirements defined in the Family Education Rights and Privacy Act (FERPA) in handling data associated with students. However, these requirements do not apply to the same type of data associated with Faculty or Staff.

Information Technology is working on a data classification policy that we believe will provide a more consistent definition for what type of University data needs to be handled as "sensitive".

The IRB office can provide guidance on how to classify the data you are collecting.

Slide 6

Some of these recommendations may be obvious (hopefully!) but represent a minimum set of steps you need to take that, when combined, will provide an acceptable level of protection against casual data interception.

Do not leave your computer logged in and unattended without logging out of your desktop session or enabling a password protected screen saver.

-Enable you screen saver to activate after 5 minutes of inactivity.

-Require a password to unlock your screensaver.

Do not lend your University laptop to your family members or friends.

Only login to your University accounts from University provided computers.

-Other home computers, libraries, etc. rarely have sufficient protection and security to protect your credentials or data.

If connecting your University provided laptop to a home wireless network, be sure your wireless setup is properly secured.

-Use a wired connection if you are unable to confirm this.

Slide 7

Passwords should be at least 9-12 characters and include a mix of upper case, lower case, numbers, and other characters. The longer the better, however:

You must be able to **MEMORIZE** your passwords or store recorded passwords in a very secure place. (No post-its stuck to the bottom of your keyboard or mouse pad!)

Consider using passphrases (which contain spaces between words) instead of passwords as they may be easier to MEMORIZE. But make sure they are also sufficiently strong.

As a generalized rule, passphrases should contain at least 6 or more words with at least 4 of the words containing at least 4 or more letters.

Do not use common phrases like "The cat jumped over the moon".

Adding upper and lower case, numbers and punctuation can make a passphrase even stronger.

Example of a very good pass phrase which could be a sentence you retrieve from your favorite book: "On July 21, 1969, Neil Armstrong became the first man on the Moon."

Avoid using the same password/phrase for multiple accounts and documents. Think "layers".

NEVER share your desktop login or NetID account credentials. **EVER.** (The IT motto: Members of the IT staff will never ask you for your NetID password.)

Slide 8

If you have administrator rights on your University provided computer, never activate services (i.e. file sharing) or install applications you are not familiar with.

If you don't know the source of a message do not reply to a request for personal information. We can guarantee:

-You did not win $274,000.23 in a foreign lottery.

-The maintenance department does not need your NetID password to update their files.

Etc! ;-)

If you don't know the source of a message do not open any attachments.

Slide 9

IMPORTANT: If you believe you have been duped or computer infected, turn your machine completely off and contact the University Help Desk or your local technical team for assistance immediately.

The sooner you report a possible compromise the more effectively you can be helped.

Slide 10

Utilize centralized file servers instead of local disk storage or email exchange

A very effective way to reduce the risk of data stolen from a desktop computer or laptop is to not store it there in the first place.

Note that while properly managed servers are very secure in and of themselves, you should still password protect your files when possible. Think "layers".

Is also a security improvement over sharing files via traditional unencrypted e-mail.

While the University's campus mail server requires SSL for data transfer security, most e-mail services across the internet do not.

Slide 11

Many office shredders available under $250 now meet the strictest government document shredding requirements. Unless you are dealing with large quantities of documents using one can be just as effective as having the documents shredded by a third party service.

Slide 12

Whole disk encryption technologies have improved significantly over the years and incur significantly less system performance degradation than in the past. However, they still remain a challenge to implement, manage and support.

Slide 13

Whole disk

Pros:

Modern implementations work more seamlessly, and are often included, with recent operating systems and incur significantly less system performance degradation than in the past.

Cons:

Can be significantly more challenging to support and integrate into desktop management solutions.

Adds an additional learning curve (and training requirement) to the user experience. In particular, proper credential management is critical.

The data encryption state is tied directly to the machine (hard disk). For example, a file encrypted on the disk is not encrypted anymore when copied to another machine or emailed.

Virtual disk encryption

Pros:

Can be as effective as whole disk encryption.

The encrypted virtual disk itself is portable so it is easier to move and support.

The data encryption state is still tied to the virtual disk. For example, a file encrypted on the virtual disk is not encrypted anymore when copied to another machine or emailed.

Cons:

Adds an even higher additional learning curve (and training requirement) to the user experience. As with whole disk, proper credential management is critical.

Effectiveness relies on the user using the virtual disk consistently and correctly. (Not as seamless as whole disk.)

Many implementations are commercial products that can be costly to implement and support at a University wide level.

Slide 14

Pros:

Ensures the secure exchange of messages and file attachments.

Enables verification of sender and message content.

Cons:

Adds an additional learning curve (and training requirement) to the user experience. In particular, proper credential management is critical.

Sender and recipient must use the same or compatible encryption tools.

Messages and attachments are only as secure as the recipient's handling of them.

Commercial products can be costly to implement and support at a University wide level .

Slide 15

Pros:

A variety of security tools and processes can be implemented to further secure client computers and protect data against theft.

Cons:

Less flexibility in the user experience.

More restrictive controls and requiring users to take additional steps (like two-factor authentication) often receive an unfortunate level of "push back" from users.

May incur an additional learning curve (and training requirement) to the user experience.

Commercial products can be costly to implement and support at a University wide level.

Slide 16

Unfortunately the perpetrators of data theft are no longer just hardcore computer hackers, possessing years of deep technical insight, looking to break into corporate or government networks in an effort to steal secret information. Personally Identifiable Information has also taken on a monetary value in data "black markets". This includes a wide range of criminals from scam artists, looking to defraud elderly persons out of their life savings, to terrorist rings looking to steal real identities in an attempt to mask their own.